CLAIMS

1. An apparatus for transmitting a file through a network, comprising:

a file-splitting processor that splits the file into a plurality of message segments and addresses the plurality of message segments to a plurality of addresses assigned to a receiving host; and

a message segment transmitter for transmitting the plurality of message segments to the receiving host.

2. The apparatus of claim 1 wherein the file splitting processor comprises a file converter that converts the file into N message segments that enable reassembly of the file from a subset of any K of the message segments, wherein N and K are positive integers, and $N > K > 1$.

3. The apparatus of claim 1 wherein the file-splitting processor further assigns a plurality of source addresses to the plurality of message segments to impede unauthorized attempts to observe the true source of a transmitted file.

4. The apparatus of claim 1 further comprising a message segment monitor for detecting non-receipt of at least one of a second plurality of message segments transmitted to the apparatus.

5. The apparatus of claim 1 further comprising an address allocator for assigning and reassigning N addresses to the receiving host.

6. An apparatus for transmitting a file through a network, comprising:

a file-splitting processor that splits the file into a plurality of message segments and assigns a plurality of source addresses to the plurality of message segments to disguise the origin of the file; and

a message segment transmitter for transmitting the plurality of message segments to a receiving host.

7. The apparatus of claim 6 wherein the file splitting processor further addresses the plurality of message segments to a plurality of addresses assigned to the receiving host.

8. A method of secure transmission of a file through a network, comprising:

(a) splitting the file into a plurality of message segments;

(b) addressing the plurality of message segments to a plurality of addresses assigned to a receiving host; and

(c) transmitting the plurality of message segments to the receiving host.

9. The method of claim 8 wherein addressing comprises addressing the plurality of message segments in one-to-one correspondence to at least a portion of the plurality of addresses.

10. The method claim 8 wherein splitting the file comprises converting the file into N message segments that enable reassembly of the file from a subset of any K of the message segments, where N and K are positive integers, and $N > K > 1$.

11. The method of claim 10 further comprising (d) assigning N addresses to the receiving host, and wherein the step of addressing comprises addressing the N message segments to the N addresses assigned to the receiving host.

12. The method of claim 11 further comprising causing the receiving host to cease receiving messages via at least

one address upon detection of an attack on the at least one address.

13. The method of claim 12 wherein the receiving host is permitted to cease receiving messages via no more than (N-K) addresses, thereby ensuring reassembly of the file by the host.

14. The method of claim 11 further comprising: (e) causing the receiving host to split a reassembled file into N message segments; and (f) causing the receiving host to transmit the N message segments from the N addresses.

15. The method of claim 8 further comprising (d) causing the receiving host to retransmit the plurality of message segments.

16. The method of claim 15 wherein the step of causing the receiving host to retransmit comprises causing the receiving host to retransmit the plurality of message segments to at least two of a plurality of hosts to relay the plurality of message segments along more than one path through the network.

17. The method of claim 8 further comprising: (d) selecting as a virtual network a plurality of hosts that includes the receiving host; and (e) assigning each one of the plurality of hosts to one of a plurality of domains, and wherein the step of transmitting comprises permitting each one of the plurality of message segments to travel to the receiving host only via relays between host pairs, each one of the host pairs selected from one of a same domain and a neighboring domain.

18. The method of claim 8 further comprising (d) assigning a plurality of source addresses to the plurality of message segments to impede unauthorized attempts to

observe a true source of a transmitted file.

19. The method of claim 8 further comprising causing the receiving host to: receive at least a portion of the plurality of message segments; reassemble the file from the received message segments; split the reassembled file into a second plurality of message segments; and transmit the second plurality of message segments.

20. The method of claim 8 wherein (c) transmitting comprises transmitting the plurality of message segments to one of an intermediate host and a destination.

21. The method of claim 8 wherein (c) transmitting comprises transmitting from one of a source and an intermediate host.

22. The method of claim 8 further comprising (d) causing the receiving host to monitor non-receipt of at least one of the plurality of message segments to detect tampering with message segment transmission.

23. The method of claim 8 further comprising: (d) assigning N addresses to the receiving host; and (e) repeatedly changing at least a portion of the N addresses.

24. The method of claim 10 further comprising (d) repeatedly changing at least a portion of the addresses assigned to the receiving host while leaving at least K of the addresses unchanged, and (e) notifying at least a portion of the network of the changed addresses, and wherein the step of addressing comprises addressing the plurality of message segments to at least the K unchanged addresses to permit continuous receipt of messages by the receiving host.

25. The method of claim 8 further comprising: (d) causing a

sending host to add status information concerning itself to the message segment; and (e) causing the receiving host to interpret the status information to detect tampering with message segment transmission.

26. The method of claim 8 further comprising (d) encoding the file to produce an encoded bit file having encoded bits, and (e) scrambling the encoded bits, and wherein the step of splitting the file splits the encoded bit file.

27. A method of secure transmission of a file through a network, comprising:

(a) splitting the file into a plurality of message segments;

(b) assigning a plurality of source addresses to the plurality of message segments to disguise the origin of the file; and

(c) transmitting the plurality of message segments.

28. The method of claim 27 further comprising (d) addressing the plurality of message segments to a plurality of addresses assigned to a receiving host.

29. A method of secure transmission of a message through a network, comprising:

(a) splitting the file into a plurality of message segments, each message segment comprising a destination specifier, protocol information and message data, the protocol information and message data being encrypted;

(b) causing a message segment to be received by a receiving host;

(c) causing the receiving host to decrypt the routing

information to determine a downstream destination host;

(d) causing the receiving host to encrypt the routing information and message data in accordance with an encryption protocol accessible to the destination host, and to transmit the thus-encrypted message segment to the destination host; and

(e) repeating steps (a)-(d) for other message segments to facilitate recovery of the message by an ultimate destination host.

30. The method of claim 29 wherein the message segment has a length, and further comprising causing the receiving host to alter the length.

31. The method of claim 29 further comprising causing the receiving host to negotiate with the destination host to determine the encryption protocol.

32. The method of claim 29 further comprising causing the receiving host to add status information concerning itself to the message segment, and causing the receiving host to interpret the status information to detect tampering with message segment transmission.

33. A method of defining and operating a network topology to camouflage network traffic patterns and volume, the network comprising a plurality of hosts, the method comprising:

(a) assigning each one of the plurality of hosts to one of a plurality of domains;

(b) permitting message transmission from each host to hosts within the domain of the host or a domain that neighbors the domain of the host, thereby defining multiple redundant relay paths among hosts; and

(c) distributing traffic across the network, thereby camouflaging message sources and destinations.

34. The method of claim 33 further comprising (d) reassigning at least one of the plurality of hosts to a different one of the plurality of domains, thereby changing network traffic patterns.

35. The method of claim 33 further comprising (d) assigning a plurality of addresses to each one of the plurality of hosts; reassigning the plurality of addresses from a pool of addresses; and notifying the plurality of hosts of the reassigned plurality of addresses.

36. The method of claim 35 wherein the step of reassigning comprises reassigning only a portion of the plurality of addresses at any one time to permit use of a remaining unreassigned portion of the plurality of addresses while notifying the plurality of hosts of the reassigned plurality of addresses.